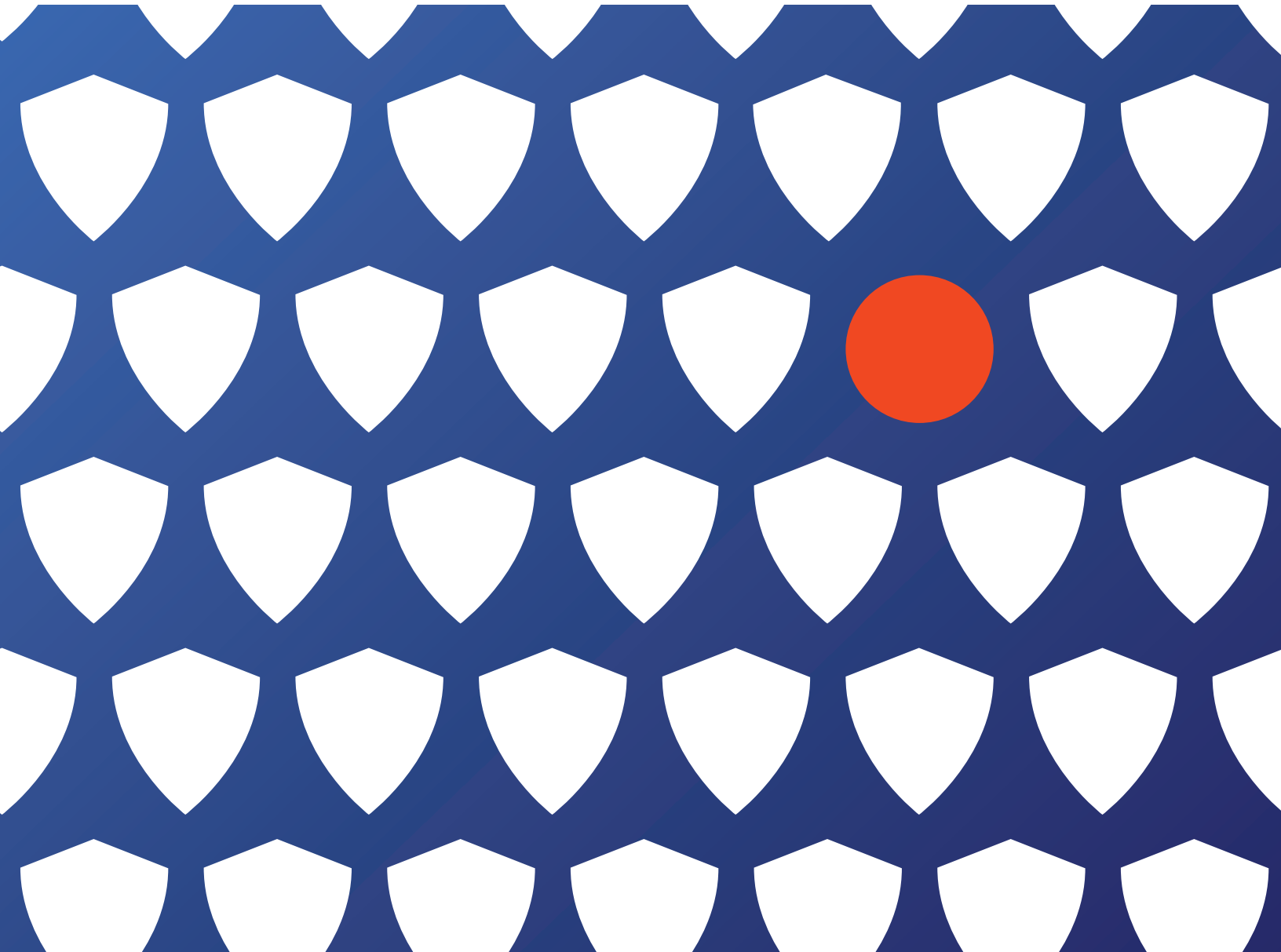
INTERPRES

WHITEPAPER

SEC Cybersecurity Regulatory Actions & The Modern CISO



The CISO and Exposure

The Job Just Changed

Recent actions by the Security and Exchange Commission (SEC) will have dramatic effects across the CISO landscape. These actions have increased the CISOs exposure to lawsuits for failing to assess, identify and manage risks and threats across their cybersecurity programs. Additionally, it exposes the CISO to employees that may disagree with the cybersecurity program and direction via the Sarbanes-Oxley Act (SOX) by empowering them to execute whistleblower activities.

Solar Winds

On 31 October 2023, the SEC announced charges against SolarWinds and its CISO for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The CISO was charged with defrauding investors by overstating SolarWinds's cybersecurity practices and understating or failing to disclose known risks.

This 68-page indictment boils down to charges of concealing the company's poor cybersecurity practices, while overstating both in word and website that the company was secure.

Reporting Requirements

On 26 July 2023, the SEC adopted rules requiring publicly traded companies to disclose material breaches of any cybersecurity incident. But more importantly, it also requires Regulation S-K item 106, to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats.

Sarbanes-Oxley

The Sarbanes-Oxley Act (SOX) was passed by the Congress of the United States in 2002 and has provisions, specifically section 404, titled "Management assessment of Internal Controls" and it extends whistleblower protections to the employees of a publicly traded company.

As a refresher, SOX 18 U.S.C. Code 1514.A.1 "...

(1) to provide information, cause information to be provided, or otherwise assist in an investigation regarding any conduct which the employee reasonably believes constitutes a violation of section 1341, 1343, 1344, or 1348, any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders..."

Impact

The impact of the SEC actions, as well as the subsequent extension of whistleblower protection to cybersecurity puts immense pressure on the modern Chief Information Security Officer (CISO), Chief Security Officer (CSO) and Business Information Security Officer (BISO) to execute a well-reasoned, defendable, and documented cybersecurity program.

Well-Reasoned and Defendable:
Material

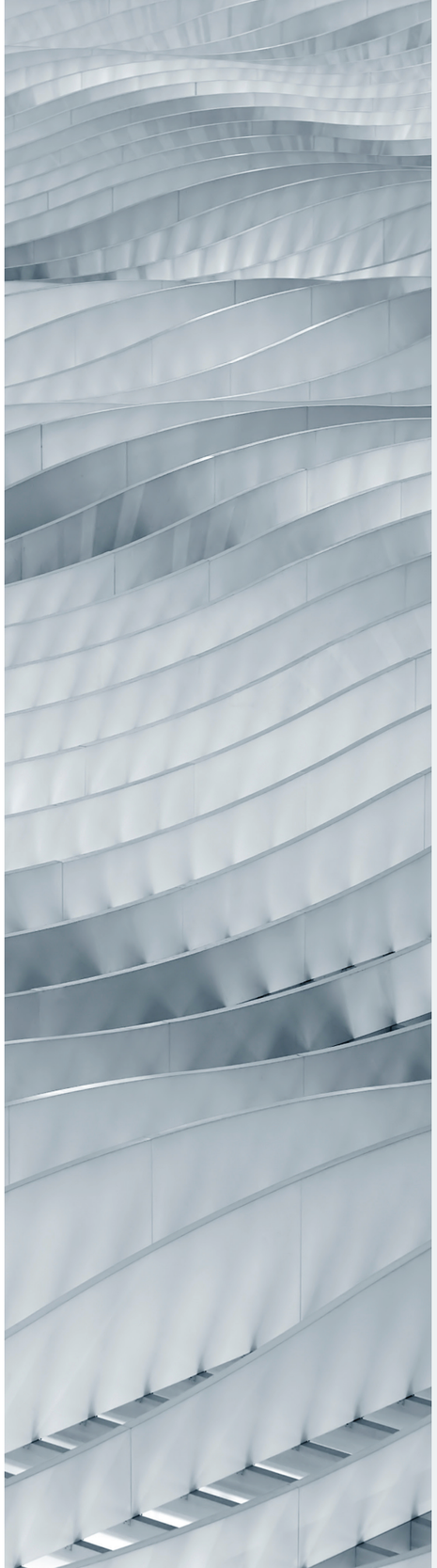
The reporting requirements under Regulation S-K Item 106 specifically call out four major activities that need to be demonstrated for a program to be well-reasoned and defendable in any subsequent litigation.

The first is ascertain what is “material.” Although cybersecurity has yet to define material risk, the SEC has provided the first rough guidelines through the SolarWinds charges. The scope of the damage to SolarWinds, The Orion software, the subsequent damage to customers under “SUNBURST”, frame the concept of what is material. In this instance, Material is equal to Impact. The CISO of today needs to have documentation of the impact of a loss or breach of the company’s networks or company’s “crown jewels”.

Well-Reasoned and Defendable:
Assessing

The second activity is assessing the threat. Within the 68-page indictment of SolarWinds, the term Threat or Threat Actor is used approximately 88 times, while risk is used 91 times. The SEC is clearly starting that threat is integral to risk and the modern CISO should heed the change to a defined set of threats versus nebulous risk scores.

There are four places the CISO should look to for intelligence on threats. Tier I Threat information is from CISA and its mission statement and function is to position itself as the authoritative source of cyber threat intelligence in the United States. Tier II includes FBI, National Security Agency/US Cyber Command, and sector specific Information Sharing and Analysis Centers (ISACS). Tier III sources are large scale commercial threat intelligence (CTI) companies and finally Tier IV is comprised of single source intelligence collection providers. The more authoritative the source (CISA) the easier it will be for the CISO to defend their actions in relation to the stated threat.



Well-Reasoned and Defendable:
Identifying

The third activity, identifying threats, provides the CISO with a well-reasoned and defendable position to start their cybersecurity program. The CISO will need to build and maintain in near-real time, the threat model of the organization. This should include size, geography, industry, infrastructure, type of data being protected, and critical assets. Using this threat model, and reporting from Tier 1 and 2 threat intelligence, the CISO will be able to define and name most-likely threat actors targeting their organization, and by extension, identify those adversaries’ techniques, tactics, and procedures. This provides the Who and How, that the cybersecurity program is actively attempting to thwart in accordance with the NIST Cybersecurity Framework (CSF) (NOTE: SolarWinds is accused of not following the NIST CSF, pg. 15, paragraph 45).

Within this activity the CISO will need to identify and prioritize vulnerabilities. Most medium to large organizations have tens of thousands of vulnerabilities spread across the organization’s infrastructure. In the SolarWinds indictment, the term “known vulnerability” is used without any context to the size and scope of the vulnerability patching activity of the organization. For the CISO any patching prioritization scheme will have to be well-reasoned and defendable. Stating a First in/First out based on CVSS score will not be defendable or even well-reasoned, when CISA produces a Known Exploitable Vulnerability (KEV) list that is roughly 30% of the known vulnerabilities. However, even a program based on KEV may not reduce the CISOs exposure, when the Forum of Incident and Response Teams (FIRST) (www.first.org) an international not-for-profit organization has identified that only 2-7% of exploited vulnerabilities are actually targeted and exploited by threat actors.

To reduce exposures, CISOs should base their prioritization schemas in the following order: 1. EPSS (first.org), 2. KEV 3. CVSS 4. Vendor warnings. Vulnerability prioritization provides the Where the adversary will attack.

Well-Reasoned and Defendable:

Managing

The fourth activity, managing the threats and vulnerabilities (e.g., material risk), is dependent on mapping relevant security controls to the Adversary (Who), their TTPs (How) and their Targets (Where). A critical step in this process is to ensure that the organization has the proper visibility and detection logic in place. Relying on the word of third-party vendors, that their product can Protect, Detect and Respond (NIST CSF), or that their product satisfies NIST 800-53 (or -171) requirements will not indemnify a CISO from SEC or a potential whistleblower. If an investigative arm (for example the Cyber Safter Review Board (CSRB) finds that a product was misconfigured or used inappropriately, the CISO will be identified as the negligent party.

Assessment Methodologies, to include Breach and Attack Simulation and Red Teaming, are especially deceptive for the modern CISO. While they have their strengths, neither uses real TTPs used by the adversaries that matter most to an organization. Rather they use the TTPs that have the widest application of use cases. Tuning a BAS or pivoting a Red Team to use the TTPs of the adversaries most likely to target you is a costly endeavor, instead CISOs can achieve the same results by maintaining a real time feed of the security environment and focusing on security entropy or “environmental drift”.

Well-Reasoned and Defendable:

Documentation and Validation

Documentation and Validation is a component of defensive readiness. Defensive readiness is ensuring that the company is prepared to defend, protect, and respond to threats that are targeting the organization. The documentation should include the company’s overall exposure to a material breach, the most-likely adversaries and their TTPs, the vulnerability prioritization schema, and finally the controls that are in place to defend, protect and respond to the threat actors most likely targeting their organization. In other words, organizations should implement a continuous threat exposure management program to validate and document their security strategy.

Well-Reasoned and Defendable:

Continuous Threat Exposure Management

Continuous Threat Exposure Management is a program designed to reduce risk by scoping the attack surface, discovering assets, prioritizing the most likely threats, validating that a vulnerability is exploitable, and the mitigation is sufficient, and finally, mobilization – ensuring that the organization is positioned to act on the remediation. Threat exposure management provides the CISO with the programmatics needed to successfully prove that their program is well-reasoned and defendable.

Establishing a comprehensive, continuous threat exposure management program, backed by Tier I and II intelligence, the modern CISO will be able to:

- Quickly determine cyber readiness through automation and analysis of defensive controls, assets, adversarial threats and vulnerabilities most likely targeting their organization.
- Streamline the analysis of defense surface tooling to comprehensively evaluate capabilities and optimize security posture in the areas of threat mitigation, visibility, and detection.
- Identify and prioritize exploitable vulnerabilities being leveraged by adversaries that target like-kind organizations.
- Identify those technologies and capabilities in your environment that do not provide value against the threats targeting you.

Interpres Security:

Built for the Modern CISO

The Interpres Threat Exposure Management platform arms the modern CISO with the ability to automatically assess, identify and manage threat exposure that defines a well-reasoned and defendable cybersecurity program.

About Interpres

Interpres Security brings context to measuring security performance with a comprehensive new perspective to managing threat exposure. In today's rapidly changing threat environment, CISO's and security teams need a data-driven and threat-informed approach to measure defensive readiness that is rapid, scalable, and automated replacing lengthy and manual processes. We capture quantifiable data to understand what current controls can detect and defend against, identify gaps, deficiencies, and misconfigurations to optimize the security stack and maximize investments.

Interpres focuses on the dynamic relationship between the defense surface, adversarial TTPs and exploitable vulnerabilities that are likely to be used to attack an organization. Using continuous situational awareness, organizations know exactly how well they are prepared for existing and breaking events, with prioritized and recommended actions to mitigate gaps and optimize defensive coverage.

Interpres Security is backed by a top cybersecurity specialist investor, Ten Eleven Ventures.

To learn more about Interpres Security visit www.InterpresSecurity.com.

Interpres Security

Published November 2023 WTP_SEC_11_2023


INTERPRES